SIMM 65D-Security Breach Involving Personal Information: Requirements and Decision-Making Criteria for State Agencies

November 2008

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

State agencies are required to operate in accordance with a myriad of laws and state policies related to the protection of information assets, and the timely and efficient management of security incidents. California's breach notification law (Civil Code section 1798.29), enacted in 2003, is one such law, intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so they could take steps to protect themselves against identity theft or to otherwise mitigate the crime's impact and other possible harms associated with a breach of personal information.

While the law originally focused on breaches involving the kind of information used in financial identity theft, growing concern about medical identity theft led to the addition of medical and health insurance information as "notice-triggering" in 2008. Safeguarding against and preventing security breaches involving personal information entrusted to government is essential to establishing and maintaining public trust. Equally important is the ability to provide accurate and timely information about a breach to affected individuals when a breach occurs because failure to do so can exacerbate the problem and increase the risk of harm to individuals.

To ensure that state agencies understand the responsibilities for making timely and accurate notification to individuals affected by a breach, this SIMM 65D document identifies the existing personal information breach notification requirements, and sets out specific instructions and guidance for state agencies to follow when responding to a security incident that involves a breach of personal information. SIMM 65D also provides a checklist and a set of breach notification templates as tools to assist agencies with fulfilling the notification requirements.

II. INTRODUCTION

To ensure compliance and consistency across state government, this document identifies the current breach notification requirements for breaches involving personal information, accompanied by questions and factors agencies should consider in determining whether and when a breach notification should be made, and a specification of the means for fulfilling notification requirements. This document does not attempt to establish an absolute standard for breach notification, since decisions are dependent upon the specific facts surrounding the breach and the applicable law. In some cases notification is clearly required by law, and in others it may be unclear whether notification is required. In some instances, where notification is, by law, clearly not required, notification may nonetheless, serve the best interests of those affected.

The procedures discussed in this document will assist agencies in confronting the problems associated with a breach involving personal information, by providing instruction and guidance regarding developing an appropriate response, understanding notification requirements, and making decisions in those cases where the obligation to notify may be uncertain.

The term "agency" refers to any office, department, board, bureau, commission or other organizational entity within state government. Within this document, "agency" and "department" are used interchangeably.

III. INFORMATION PRACTICES ACT REQUIREMENTS

A. Background

The California Information Practices Act (IPA) of 1977 (Civil Code sections 1798 et.seq) is the primary authority that governs state agencies' collection, use, maintenance, and dissemination of individuals' personal information. The IPA also specifies the circumstances that compel breach notification.

For the general purposes of the IPA, California Civil Code section 1798.3 defines personal information very broadly as "any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, Social Security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual."

B. Breach Notification Requirement

Subdivision (a) of Civil Code section 1798.29, requires "Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The breach notification section of the IPA, (subdivision (e) of Civil Code section 1798.29, more narrowly defines, "personal information" as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social Security number.
(2) Driver's License number or California Identification Card number.
(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(4) Medical information (as defined).
(5) Health insurance information (as defined).

Subdivision (f) of Civil Code Section 1798.29 specifically defines personal information, medical information, and health information for purposes of this section as follows:

(1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. (Note; however, personal information held in public records, or portions thereof, may need to be redacted prior to disclosure to comply with Civil Code section 1798.24).

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

For purposes of this document the elements of personal information described in subdivisions (e) and (f) of Civil Code section 1798.29 are hereinafter referred to as "notice-triggering" data elements.

IV. STATE POLICY REQUIREMENTS

A. Information Processing Standards

State policy, in accordance with State Administrative Manual (SAM) section 5100, requires state agencies to use the American National Standards Institute (ANSI) management information standards and the Federal Information Processing Standards (FIPS) in their information management planning and operations. The ANSI standards are national consensus standards that provide guidance on a variety of issues central to the public and industrial sectors. Under the Information Technology Management Reform Act (Public Law 104-106). The Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) as FIPS for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

In relation to Civil Code section 1798.29's exemption from the breach notification requirement for a breaches involving encrypted notice-triggering information, this requirement, includes without limitation, those NIST standards related to the validation of cryptographic modules found in **encryption products used in the protection of confidential, personal, or sensitive information.** The exemption is only applicable to those incidents involving data encrypted with products validated by NIST as FIPS 140-2 compliant.

B. Incident Management

State policy (SAM section 5350) requires agency management to promptly investigate incidents involving loss, damage, misuse of information assets, unauthorized access, or improper dissemination of information, and immediately report the occurrence of such incidents to the California Highway Patrol's (CHP's) Emergency Notification and Tactical Alert Center (ENTAC) at (916) 657-8287.

Proper incident management includes the formulation and adoption of an incident management plan that provides for the timely assembly of appropriate staff that are capable of developing a response to, appropriate reporting about, and successful recovery from a variety of incidents. In addition, incident management includes the application of lessons learned from incidents, together with the development and implementation of appropriate corrective actions directed to preventing or mitigating the risk of similar occurrences.

In conjunction with the aforementioned requirements, state policy (SAM Section 5350.4) requires every state agency that collects, uses, or maintains personal information to include in their incident management plan, procedures for responding to a security breach involving personal information **regardless of the medium in which the breached information is held** (e.g., paper, electronic, oral, or the combination of data elements involved including non-notice-triggering personal information). These procedures must be documented and must address, at a minimum, the following:

1. Agency Incident Response Team. An agency's procedures shall identify the positions responsible for responding to a security breach involving personal information. An agency's response team must include, at a minimum, an escalation manager, the Program Manager of the program or office experiencing the breach, the Information Security Officer (ISO), the Chief Privacy Officer/Coordinator (CPO) or Senior Official for Privacy, the Public Information or Communications Officer, Legal Counsel, and a representative from the Office of Information Security and Privacy Protection (OISPP). The escalation manager, often the ISO or CPO, is responsible for ensuring appropriate representatives from across the organization are involved, and are driving the process to completion. Some incidents will require the involvement of other persons not mentioned above. For example, if the source of the compromised information was a computer system or database, the Chief Information Officer should also be involved in the response activity. As another example, if the incident involves unauthorized access, misuse, or other inappropriate behavior by a state employee, or the security breach involves a compromise of state employee's personal information, the Personnel Officer or Human Resources Manager should also be involved in the response activity. Further, if the incident involves multiple agencies, the response team from each agency may be involved.

2. Protocol for Escalation and Internal Reporting. An agency's procedures shall outline the method, manner, and progression of internal reporting, so as to ensure that the agency's executive management is informed about the breach of personal information, the Agency Incident Response Team is assembled, and the incident is addressed in the most expeditious and efficient manner.

3. Protocol for Security Incident Reporting. Any actual or suspected breach of personal information (notice-triggering and non-notice-triggering data elements) in any type of media (e.g., electronic, paper) is to be reported immediately to the CHP's ENTAC at (916) 657-8287. This telephone number is staffed 24-hours a day, seven days a week. The officers at ENTAC will require specific information about the incident and will forward that information to the OISPP Office of Information Security and to the CHP Computer Crimes Investigation Unit (CCIU). An agency should inform the officer taking the report that the incident involves a personal information breach and the type of media involved (e.g., electronic, paper, both electronic and paper, etc.). Representatives from the Office of Information Security and CCIU will contact the agency as soon as possible following their receipt of the ENTAC report.

   Reporting to law enforcement is also an important way for an agency to mitigate the risks faced by the affected individuals, because those entities are able to coordinate with appropriate federal law enforcement agencies and identity theft

task forces, to look for potential links and effectively investigate and punish criminal activity that may result from, or be connected to, a breach.

IMPORTANT: A report made to CHP, other law enforcement agencies, or the OISPP outside of the ENTAC notification process by email or other means is NOT an acceptable substitute for the required report to ENTAC.

Unless otherwise directed by OISPP, a follow-up written report is to be completed and submitted to the OISPP within ten (10) business days from the date an incident is first reported. The Agency Security Incident Report (SIMM 65C) form is to be used to submit this report.

4. Decision-Making Criteria and Protocol for Notifying Individuals.
Both the decision to provide external notification on the occasion of a breach and the nature of the notification will require agencies to resolve a number of questions. An agency's procedures shall include documentation of the methods and manner for determining when and how notification is to be made.
To assist agencies with navigating the decision-making process, a checklist is provided as Appendix A, Breach Response and Notification Assessment Checklist.

   The procedures shall, at a minimum, address the following elements:

   a. Whether the notification is required by law.
   b. Whether the notification is required by state policy.
   c. Timeliness of notification.
   d. Source of notice.
   e. Content of notice.
   f. Approval of notice prior to release.
   g. Method(s) of notification.
   h. Preparation for follow-on inquiries.
   i. Other actions that agencies can take to mitigate harm to individuals.
   j. Other situations when notification should be considered.

A more detailed description of these elements is set forth in the following section.

V. ESSENTIAL ELEMENTS TO CONSIDER

A. Whether Breach Notification Is Required by Law

California's Breach Notification Law (California Civil Code section 1798.29) requires "Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

The law is intended to give individuals early warning when their personal information is reasonably believed to have been acquired by an unauthorized person, so that those individuals can take steps to protect themselves against identity theft or to otherwise

mitigate the crime's impact. While the law originally focused on breaches involving the kind of information used in financial identity theft, growing concern about medical identity theft led, in 2008, to the addition of medical and health insurance information as notice-triggering information.

To determine whether notification of a breach is required by law, the agency should consult with their legal counsel. However, answering the following questions should assist the agency and its legal counsel in making this determination:

1. Was computerized data owned or licensed by the state agency involved?

   When determining whether or not the incident involved computerized data, the agency is to consider, at a minimum, whether the data involved was processed or stored with or in a computer or computer system. This includes, but is not limited to, copier, facsimile and business hub machines, mobile telephone and portable digital assistant (PDA) devices, and data processed or stored with or in electronic mail systems.

2. Was a computer system, or computer peripheral, or storage device with the capability of storing computerized data owned or licensed by the state agency involved?

   When determining whether or not the incident involved a computer system, or computer peripheral, or storage device with capability of storing computerized data the agency is to consider the wide array of data storage devices available today. This includes, but is not limited to, those mentioned above, as well as USB flash, jump or pen drives, CDs and DVDs, external and removable hard drives, and magnetic and optical backup tapes/disks.

3. Were notice-triggering data elements involved?

   In accordance with subdivisions (e) and (f) of Civil Code section 1798.29, notice triggering data elements include an individual's first name or first initial and last name in combination with any one or more of the following:

   a. Social Security number.
   b. Driver’s License number or California Identification Card number.
   c. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
   d. Medical information (as defined).
   e. Health insurance information (as defined)

4. Were the notice-triggering data elements encrypted using FIPS 140-2 validated or NIST certified cryptographic modules?

   The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standards (FIPS 140-2 and others). Agencies may consult NIST’s CMVP website at http://csrc.nist.gov/groups/STM/cmvp/validation.html for an alphabetical list of vendors who have implemented NIST validated cryptographic modules. For more

information about state adopted standards refer to Standards on the OISPP Go RIM website at http://www.oispp.ca.gov/government/go_rim/go_RIM-section5345.asp

FIPS 140-2 precludes the use of invalidated cryptography **for the cryptographic protection** of sensitive or valuable data. Invalidated cryptography is viewed by NIST as providing **no protection** to the information or data - in effect the data would be considered unprotected plaintext.

5. Were the notice-triggering data elements acquired, or reasonably believed to have been acquired by an unauthorized person?

   When determining whether or not acquisition has actually or is reasonably believed to have occurred, an agency is to consider, at a minimum, the following indicators:

   a. The information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other devices that have the capability of containing information, or such as a misdirected electronic mail transmission received and opened by an unauthorized person containing notice-triggering information.
   b. The information has been downloaded or copied (e.g., any evidence that download or copy activity has occurred which may require forensic analysis);
   c. The attacker deleted security logs or otherwise "covered their tracks";
   d. The duration of exposure in relation to maintenance of system logs or in cases of an inadvertent or unauthorized Web site posting;
   e. The attack vector is known for seeking and collecting personal information;
   f. The information was used by an unauthorized person, such as instances of identity theft reported or fraudulent accounts opened.

B. Whether Breach Notification Is Required by State Policy

The compromise of notice-triggering data elements found in physical information systems poses the same level of risk to individuals as a compromise of notice-triggering data elements found in computerized systems; thus, state policy requires notification be made to individuals in these cases, as well. To determine whether notification is **required** by state policy, the agency should still consult with its legal counsel. However, answering the following questions, which are a slight variation to those above, should assist the agency and its legal counsel in making this determination:

1. Was data, on **any other media type or format** (e.g., paper, cassette tape), owned or licensed by the state agency involved?

2. Were notice-triggering data elements involved?

   In accordance with subdivisions (e) and (f) of Civil Code section 1798.29, notice triggering data elements include an individual's first name or first initial and last name in combination with any one or more of the following:

a. Social Security number.
b. Driver's License number or California Identification Card number.
c. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
d. Medical information (as defined).
e. Health insurance information (as defined)

3. Were the notice-triggering data elements acquired, or reasonably believed to have been acquired by an unauthorized person?

When determining whether or not acquisition has actually or is reasonably believed to have occurred, an agency is to consider the following indicators:

a. The information is in the physical possession and control of an unauthorized person, such as a misdirected, lost, or stolen hardcopy document, or file containing notice-triggering information. This includes, but is not limited to, documents containing notice-triggering data elements which have been addressed and mailed to an unauthorized person, transmitted by facsimile to an unauthorized person, or information containing notice-triggering data elements which is otherwise conveyed, such as by word-of-mouth, to unauthorized persons.
b. The information has been viewed, acquired, or copied by an unauthorized person, or a person exceeding the limits of their authorized access.
c. The information has been shared by an unauthorized person or was used by an unauthorized person, such as instances of sharing the personal information with the media or tabloids, or identity theft reported, or fraudulent accounts opened.

C. Timeliness of the Notification

Following the discovery of a breach that involves personal information which meets the statutory or policy criteria for notification, agencies should provide notification to affected individuals in a timely manner and without unreasonable delay. To the extent possible, notification should be made within ten (10) business days from the date the agency has determined that the information was, or is reasonably believed to have been, acquired by an unauthorized person. The following are examples of circumstances which may warrant the delay of notification beyond the 10 days following discovery:

- Legitimate needs of law enforcement, when notification would impede or compromise a criminal investigation, or pose other security concerns (Civil Code section 1798.29 (c).

- Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system, so that the harm of the initial incident is not compounded by premature announcement. For example, if a data breach resulted from a failure in a security or information system, that system should be repaired and tested before disclosing details related to the incident. (Civil Code section 1798.29 (a).

Any decision to delay notification should be made by the agency head, or the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf, and any delay should not exacerbate the risk or harm to any affected individual(s).

D. Source of the Notice

Given the serious security and privacy concerns raised by breaches involving personal information, the notice to individuals affected by the loss should be issued and signed by a responsible official of the agency. In those instances in which the breach involves a widely known component of an agency, notification should be given by a responsible official of the component. In general, notification to individuals affected by the breach should be issued by the agency head, or by the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf. Such action, demonstrates that the incident has the attention of the chief executive of the organization.

There may be some instances in which notice of a breach may appropriately come from an entity other than the actual agency that suffered the loss. For example, when the breach involves a contractor operating a system of records on behalf of the agency or a public-private partnership. The roles, responsibilities, and relationships with contractors or partners for complying with notification procedures should be established in writing with the contractor or partner prior to entering the business relationship, and must be reflected in the agency's breach response plan and in the contractual agreements with those entities.

Whenever practical, to avoid creating confusion and anxiety for recipients of the notice, the notice should come from the entity that the affected individuals are more likely to perceive as the entity with which they have a relationship. In all instances, when the breach involves a contractor or a public-private partnership operating a system on behalf of the agency, the agency is responsible for providing any required or necessary notification, and for taking appropriate corrective actions.

E. Content of the Notice

The substance of the notice should be written in clear, concise, and easy-to-understand language. The notice should avoid the use of technical jargon and include, at a minimum, the following elements:

1. A general description of what happened. Agencies should be mindful of the impact of disclosing either an insufficient amount of detail or too much detail in the general description of what happened. For example, in cases where an investigation is ongoing, disclosing certain details may impede or compromise the investigation, or cause other security concerns. On the other hand, failure to disclose a sufficient amount of detail may not provide the recipient with enough information to fully understand and mitigate their own risk. An agency must work with law enforcement authorities to ensure the content strikes the necessary balance.

2. A description of the type of personal information involved in the breach (e.g., full name, Social Security number, Drivers License number, California Identification Card number, date of birth, home address, account number, disability code, medical or health information (as defined), etc.). The specific type of notice-triggering data elements are to be provided in the notice. This is extremely important in order to help the recipient of the notice to fully understand how to mitigate their risk.

3. All of the steps that the individual could take to protect themselves from potential harm, if any.

4. An apology and a description of the steps the agency is taking, has taken, or will take, to investigate the breach, mitigate any losses, and protect against any further breaches.

5. The name of the individual contact(s) at the agency with the ability to provide more information about the breach to the affected individuals.

6. A toll-free telephone number for the agency contact, physical address, e-mail address, and postal address if available. If the agency does not have a toll-free telephone number a local telephone number may be provided.

When the agency has knowledge that the affected individuals are not English speaking, to the extent practical, the notice should also be provided in the appropriate language(s). Given the amount of information required above, in cases where it is only the name and Social Security number that has been breached, agencies may want to consider using the one-page *Security Breach First Steps* document as an enclosure with the notice letter. It is available in both English and Spanish and can be downloaded from the OISPP Web site at http://www.oispp.ca.gov/consumer_privacy/pdf/Security_Breach_First_Steps.pdf

The *Security Breach First Steps* document, as well as standardized breach notification templates for breaches involving other notice-triggering information, is provided as appendices in this document. In some cases it may be necessary to combine the language from multiple templates, such as in the hybrid template provided.

Consistent with Section 504 of the Rehabilitation Act of 1973, the agency should also give special consideration in providing notice to individuals who are visually or hearing impaired. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the agency's Web site.

F. Approval of the Notice

State policy (SAM Section 5350.4), requires state agencies to submit draft breach notices to the Office of Information Security and Privacy Protection (OISPP) for review and approval **prior to their release**. The intent is to ensure the consistency and clarity of notices, as well as the accuracy of privacy protection steps and instructions provided in notices. The procedures for submitting a request for review and approval of a draft breach notice to the OISPP are as follows:

1. Submit by e-mail attachment to Security@oispp.ca.gov or by facsimile by obtaining the facsimile number before transmitting the facsimile.

2. Communicate with an OISPP Security representative by telephone at (916) 445-5239 immediately prior to submission of any document, in order to alert the Office that a document requiring review will soon arrive.

3. Indicate the target date of release. Allow at least one full business day for OISPP's review and approval of the initial and any subsequent submittals that are necessary due to changes not previously reviewed and approved by OISPP.

4. Mark the submittal as urgent and include the following information:
    a. "Request for OISPP Review and Approval of Draft Breach Notice" contained in the subject line of the e-mail message or the facsimile transmission cover sheet;
    b. The OISPP incident tracking number;
    c. The anticipated or desired date for release to individual(s); and
    d. The name and contact information of the agency employee capable of responding to OISPP questions about the draft notice.

Prior to release to any individual, the final breach notice is to be submitted to OISPP according to the following procedures:

1. Submit by e-mail attachment to Security@oispp.ca.gov or facsimile by obtaining the facsimile number prior to submittal.

2. Include all of the following information in the submittal:
    a. "Final Breach Notice" to be included in the subject line of the e-mail message or the facsimile transmission cover sheet;
    b. The OISPP incident tracking number; and
    c. The name and contact information for the person(s) capable of responding to OISPP questions about the notice.

Depending on the circumstances, the agency may also need to contact other public and private sector agencies, particularly those that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach. For example, an agency may need to seek confirmation from law enforcement that notification will not compromise the investigation. Or, when as a result of a large breach in individual names and Driver's License numbers, the agency intends to reference the Department of Motor Vehicle (DMV) Fraud Hotline in the notice; the agency should seek DMV's approval and provide DMV with advanced warning that DMV may experience a surge of inquiries.

G. Method(s) of Notification

The best means for providing notification will depend on the nature and availability of contact information of the affected individuals, as well as the number of individuals affected. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The following are examples of the types of notification which may be considered.

1. First-Class Mail. Written notice to the named individual, whenever possible by first-class mail to the last known address in the agency's records, should be the primary means of notification. For example, the notice should be addressed to "Jane Doe", and in cases of minor children the notice should be addressed "To the Parent of: Jane Doe". Where there is reason to believe the address is no longer current, an agency should take reasonable steps to update the address by consulting with other agencies, such as the U.S. Postal Service (USPS). The USPS will forward mail to a new address, or will provide an updated address via established processes. The notice should also be sent separately from any other mailing so that it stands out to the recipient, and it should be labeled to alert the recipient to the importance of its contents, (e.g., "Important Information Enclosed"), and as to reduce the possibility that it may be mistaken as advertising mail.

2. Telephone. Notification by telephone may be appropriate as a supplement to written notice in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. Persons making the notification by telephone should only do so by personal contact with the affected individual, and never through a message on answering machine or other parties. In all cases, written notice by first-class mail must also be made concurrently.

3. E-Mail. E-mail notification is problematic, because individuals change their e-mail address and often do not notify all parties of the change, and it may be difficult for individuals to distinguish the agency's e-mail notice from a "phishing" e-mail. Furthermore, the breach notification law allows email notice only as consistent with the federal Electronic Signatures Act (15 U.S. Code 7001). The Electronic Signatures Act requires, among other things, that an agency must have received express consent from the individual to use e-mail as the primary means of communication before making the breach notification.

4. Substitute Notification. Subdivision (g), (3) of Civil Code section 1798.29, provides for substitute notification when an agency can demonstrate that more than 500,000 individuals were affected, or the cost of providing notification would exceed $250,000, or the agency does not have adequate contact information on those affected. In accordance with that provision of law, substitute notification consists of **all** of the following methods:

    a. Conspicuous posting of the notice on the agency's Web site, if the agency maintains a Web site; and
    b. Notification to major statewide media; and
    c. E-mail notification when the agency has an e-mail address for the individuals. Here, because an agency is also doing a. and b., the e-mail notice does not need to meet the requirements of the Electronic Signature Act.

    When posting breach information on the agency's Web site, the posting should be made on the home page or provided as a clearly identifiable link from the agency's home page. The posting should also include a link to Frequently Asked Questions (FAQs) and other talking points to assist the public's understanding of

the breach and notification process. See the FAQ template provided on the OISPP Web site at the following link: http://www.oispp.ca.gov/government/privacy/documents/doc/security_breach_faqs.doc. The FAQ template should be modified as appropriate to fit the facts of the incident.

Further, when making a substitute notification, the public media should be notified as soon as possible after the discovery of the breach because delayed notification may erode public trust. However, an agency's decision to notify the public media in conjunction with substitute notification, or in other situations, will require careful planning and execution so that the agency is adequately prepared to handle follow-on inquiries.

H. Preparation for Follow-on Inquiries from Noticed Individuals

Those affected by the breach can experience considerable frustration if, in the wake of the individual notification or the initial public announcement, they are unable to find sources of additional accurate information. This applies to both follow-on inquiries made to the agency that experienced the breach, as well as to counterpart entities that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach. For example, depending upon the nature of the incident and the information involved, certain entities, such as the credit-reporting agencies, may also need to prepare for a surge in inquiries that might far exceed normal workloads (e.g., requests for copies of credit reports and posting of fraud alerts).

Consequently, and as appropriate, agencies must adequately prepare for follow-on inquiries and must address inquiries in the most efficient and accurate manner possible. In doing so, an agency should consider provisioning for the following:

1. Instructions to each of its public inquiry intake units about where they should direct both telephone and in-person inquiries about the breach from affected individuals, the media, and the public.

2. A toll-free phone line, answered by personnel specifically trained to handle inquiries from affected individuals and the public, especially when the breach has affected a large number of individuals.

   Documented scripts, and answers to anticipated and frequently asked questions (FAQs). Refer to the FAQ template provided on the OISPP Web site at the following link: http://www.oispp.ca.gov/government/privacy/documents/doc/security_breach_faqs.doc. The FAQ template should be modified as appropriate to fit the facts of the incident.

3. A complaint resolution and/or escalation process. For example, individuals may be directed to the agency's Office of Civil Rights, if one is available.

4. Early warning and information about the timing of notification to all counterpart entities, so that they may adequately prepare for any potential surge in inquiries.

5. The timing for delivery of the notice to noticed individuals in conjunction with the availability of staff to respond to follow-on inquiries must also be considered. For example, an agency should not release a notification so that it is likely to be received on the last work day before major holiday weekend or the day of an observed holiday.

The OISPP can assist agencies with the development of scripts, FAQs, staff training and other related notification activities.

I. Other Situations When Breach Notification Should Be Considered

Neither state law nor state policy requires notification in the case of breaches involving non-notice-triggering personal information. Nevertheless, breaches involving certain types of non-notice triggering personal information can also implicate a broad range of harms to individuals. The other types of harm that an agency should consider, depending upon the nature of the personal information involved, and the circumstances of the loss or theft, include but are not limited to, the following:

- Harm to reputation.
- Potential for harassment.
- Potential for prejudice, particularly when health or financial benefits information is involved.
- Other types of financial loss, such as an increase or denial of insurance premiums which may be associated with the latter.
- Embarrassment.
- Legal problems.

In situations where other (non-notice-triggering) personal information is involved, an agency should, in consultation with its legal counsel and the OISPP, consider the following factors when making an assessment of the likely risks of harm and the decision to notify:

1. Nature of the Data Elements Breached. The nature of the compromised data elements is a key factor to consider in determining if notification should be provided to affected individuals. It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive in another context. For example, the breach of a list containing the names and home addresses of undercover peace officers or domestic violence victims, poses a higher risk of harm than a list containing the names of individuals that subscribe to an agency's monthly newsletter on general family issues. Yet in the context of this subscriber list, if the newsletter were specific to a certain profession or clientele it could pose a higher level of risk, such as a newsletter that is specific to a support group for battered persons. It is also important to note that a Social Security number alone is useful in committing identity theft. In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of possible harms that could result from their acquisition by or disclosure to unauthorized individuals.

2. Likelihood the Information Is Accessible and Usable. Upon learning of a breach, agencies should assess the likelihood that personal information will be or has been acquired and misused by unauthorized individuals. An increased risk that the information will be misused by unauthorized individuals should influence the agency's decision to provide notification.

   The fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals; however, depending upon any number of physical, technological, and procedural safeguards employed by the agency, the risk of compromise may be low to non-existent. For example, exposure on a public website for many weeks or months would increase the likelihood that it was acquired by an unauthorized individual. Also if the information was properly protected by encryption then the likelihood the information is accessible and usable is non-existent; whereas, "paper copies" of printed personal information are essentially unprotected and would be considered a much higher risk of compromise depending upon the type of information involved.

   In this context, the encryption product and algorithm used has been validated by the National Institute of Standards and Technology (NIST) to the American National Standards Institute (ANSI) management information standards and the Federal Information Processing Standards (FIPS), as state agencies are required to use the ANSI and FIPS standards in their information management planning and operations (SAM Section 5100).

3. Likelihood the Breach May Lead to Harm. The IPA (Civil Code section 1798.21) requires agencies to protect against anticipated threats or hazards to the security or integrity of records containing personal information which could result in any injury to individuals. When considering injury to individuals, agencies should consider the broad reach of potential harm and the likelihood harm will occur.

   a. *Broad Reach of Potential Harm.* The number of possible harms associated with the loss or compromise of information may include, but are not necessarily limited to, the following:

      i. the effect of a breach of confidentiality or fiduciary responsibility;
      ii. the disclosure of address information for victims of stalking or abuse, or persons in certain high risk professions (e.g., law enforcement officers, reproductive health care clinic workers, etc.);
      iii. legal problems (e.g., an individual uses another individual's name and Drivers License number when arrested, or a pregnant woman uses the medical identity of a mother and delivers a baby who tested positive for illegal drugs. Consequently, Social Services takes her children from her and she must hire an attorney to prove that she is the victim of medical identity theft);
      iv. harm to reputation;
      v. financial loss;
      vi. the disclosure of private facts and unwarranted exposure leading to embarrassment, humiliation, mental pain, emotional distress, or loss of self-esteem;

vii. the potential for secondary uses of the information which could result in fear or uncertainty; or
viii. the potential for harassment, blackmail, or prejudice, particularly when health or financial benefits information is involved.

b. *Likelihood Harm Will Occur*. The likelihood that a breach of non-notice triggering personal information may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. While not considered notice-triggering under the law, a Social Security number alone is useful in committing identity theft, and if there is evidence that this information was the specific target of attack by a known identity theft fraud ring, the likelihood of harm would be considered greater than if this same information had been inadvertently exposed or acquired.

4. Ability of the Agency to Mitigate the Risk of Harm to Individuals. Within an information system, the risk of harm will depend on how the agency is able to mitigate further compromise of the system(s) and/or information affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken. For example, if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address may signal fraudulent activity.

   The ability of an agency or other affected entities to monitor for and prevent attempts to misuse the compromised information is a factor in determining the risk of harm, particularly the harms associated with identity theft. Such mitigation may not prevent the use of personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

   Where practical, the agency should exhaust its ability to mitigate any risk of harm, and provide timely instruction and guidance in the notice to affected individuals about steps they can take to protect themselves.

5. Ability of the Notified Individuals to Mitigate the Risk of Harm to Themselves. Notification should be designed to afford affected individuals an opportunity to mitigate their risk. For example, in the case where the name and home address of a victim of abuse has been compromised, the individual may, in order to mitigate their risk, choose to move or to affect a greater situational awareness.

   In some cases the apology and assurance of corrective action, addressed through notification, may serve as a satisfactory remedy for those individuals who have been impacted, or potentially impacted, by the breach.

   On the other hand, agencies should bear in mind that notification, when there is little or no risk of harm might create unnecessary concern and confusion. Additionally, under circumstances where notification could increase the risk of harm, the prudent course of action is not to notify.

J. Other Actions That Agencies Can Take to Mitigate Harm to Individuals

In addition to notifying affected individuals, it may be necessary for an agency to take other actions to mitigate the risk of harm. For example, if the breach involves government credit cards, the agency should notify the issuing bank promptly; or, if the breach is likely to lead to benefit fraud (e.g., Medi-Cal, Unemployment Insurance, etc.), the agency should notify the benefit agency, so that they can take appropriate actions, such as flagging accounts associated with the affected individuals.

VI. OTHER CONSIDERATIONS

Outside of the legal and policy requirements discussed earlier there are two other steps an agency may consider to mitigate the affects of a breach on the agency and the individuals. The first is advanced notification to the media and the second is credit monitoring services. These are discussed in more detail below.

A. Advance Notification to the Media

Though not required, in breaches likely to receive greater attention, an agency may consider providing advance notification to the media as notifications are mailed to individuals. This allows the agency to present the facts of the story first, rather than trying to correct inaccurate or incomplete news stories after they are published. Advance notification to the media also demonstrates openness and can promote good ongoing communications with reporters. In addition, providing accurate information through the news media is another way to reach those affected and to explain what steps they can take to protect themselves.

As mentioned above, the timing of any notification to media or individuals is critical. The agency must ensure it is prepared to handle follow-on inquiries and is appropriate given the circumstances. In some cases, it may be more prudent not to notify news media at the same time notification is made to affected individuals. For example, an individual who has stolen a password-protected laptop in order to resell it may be completely unaware of the nature and value of the information the laptop contains, and may wipe the laptop clean before selling it. In such a case, public announcement may actually alert a thief to what he possesses, increasing the risk that the information will be misused, and it would be wise to delay media notification at least until affected individuals have received notice and had time to take defensive action.

B. Credit Monitoring Services

The offer of credit monitoring services can provide an additional measure of protection for individuals affected by a breach - especially where the compromised information presents a risk of new accounts being opened. However, this involves agency expense and the services are only useful in cases where there has been a breach of Social Security number, California Drivers License, or California Identification Card number.

Credit monitoring is a commercial service that cannot prevent or guarantee that identity theft will not occur; however, it can assist individuals in early detection of instances of new-account identity theft, thereby allowing them to take steps to minimize the harm. Typically, the service notifies individuals of activities on their credit files, such as creation

of a new account or inquiries to the file. Various services provide different features and are constantly evolving, so it is best to consult with the OISPP when and if an agency is considering providing a credit monitoring option. OISPP can provide recommendations on contract terms and how to explain the enrollment process to individuals.

VII. APPENDICES

To assist the agency with responding to a breach and drafting a breach notice the following breach response checklist, and the sample breach notices and the corresponding document enclosure has been provided as appendices herein**. Note: If a breach involves more than one type of notice-triggering information, the notice should use language from <u>all</u> the relevant sample notices.**

Appendix A: Breach Response and Notification Assessment Checklist

Appendix B: Sample Breach Notice - Social Security Number

Appendix C: Sample Breach Notice - Driver's License or California ID Card Number

Appendix D: Sample Breach Notice - Credit Card Number or Financial Account Number

Appendix E: Sample Breach Notice - Medical Information

Appendix F: Sample Breach Notice - Health Insurance Information

Appendix G: Sample Breach Notice - Hybrid

Appendix H: Security Breach - First Steps Enclosure (English)

Appendix I: Security Breach - First Steps Enclosure (Spanish)

A. APPENDIX A: Breach Response and Notification Assessment Checklist

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 65D Reference	Yes	No	Notes/Comments
1. Assemble Agency Response Team	p. 6			
1.1. Escalation Manager/Team Lead	p. 5			
1.2. Program Manager (office experiencing the breach)	p. 6			
1.3. Information Security Officer	p. 6			
1.4 Chief Privacy Officer or Coordinator	p. 6			
1.5 Public Information Officer or Communications Officer	p. 6			
1.6 Legal Counsel	p. 6			
1.7 Personnel Officer or Human Resource Manager	p. 6			
1.8 Chief Information Officer or Technology Specialist	p. 6			
1.9 Other	p. 6			
2. Escalation/Internal Reporting	p. 6			
2.1 Deputy Director	p. 6			
2.2 Director	p. 6			
2.3 Agency Secretary	p. 6			
2.4 Governor's Office	p. 6			
2.5 Other	p. 6			
2.6 Other	p. 6			
3. Security Incident Reporting	pp. 6 and 7			
3.1. Reported to CHP ENTAC at (916) 657-8287	pp. 6 and 7			
3.2. Respond to CHP CCIU response inquiry	pp. 6 and 7			
3.3. Respond to OISPP response inquiry	pp. 6 and 7			
3.4. Prepare and submit follow-up written report (SIMM 65C) to OISPP	pp. 6 and 7			
4. Is an assessment meeting necessary?				
4.1. Agency Response Team Members to Attend				
4.2. OISPP Response Team Member to Attend				
4.3. CCIU Response Team Members to Attend				
4.4 Other				

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 65D Reference	Yes	No	Notes/Comments
4.5 Other				
4.6 Sign in Sheet / Attendee roster needed				
4.7. Non-disclosure agreement forms needed				
5. Is breach notification required by law (Civil Code Section 1798.29)?	p. 8			
5.1. Was computerized data owned or licensed by the agency involved?	p. 8			
5.2. Was a computer system, equipment, or peripheral storage device (capable of containing computer data) involved?	p. 8			
5.3. Were notice-triggering data elements involved?				
5.3.1. First name or first initial and last name, and one or more of the following:	pp. 4 and 8			
5.3.2. Social Security number	pp. 4 and 8			
5.3.3. California Driver's License or Identification Card number	pp. 4 and 8			
5.3.4. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.	pp. 4 and 8			
5.3.5. Medical information (as defined)	pp. 4 and 8			
5.3.6. Health insurance information (as defined)	pp. 4 and 8			
5.4. Were the notice-triggering data elements encrypted?				
5.4.1. Was the encryption product used, a FIPS -140 validated or NIST certified cryptographic module?	p. 9			
5.5. Were notice triggering data elements acquired, or reasonably believed to have been acquired by an unauthorized person? ***(Examples only-list is not limited to these***)	pp. 8 and 9			
5.5.1. The system, equipment, or information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other devices that have the capability of containing information.	p. 8			
5.5.2. The information is has been downloaded or copied (e.g., any evidence that download or copy activity has occurred)	p.9			
5.5.3. The attacker deleted security logs or otherwise "covered their tracks".	p. 9			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 65D Reference	Yes	No	Notes/Comments
5.5.4. The duration of exposure in relation to maintenance of system logs or in cases of an inadvertent or unauthorized Web site posting.	p. 9			
5.5.5. The attack vector used is known to seek and collect personal information	p. 9			
5.5.6. The information was used by an unauthorized person, such as instances of identity theft reported or fraudulent accounts opened.	p. 9			
6. Is breach notification required by state policy (SAM sections 5350.2 and 5350.5)?	p. 9			
6.1. Was data, of any media type or format (e.g., paper), owned or licensed by the agency involved?	p. 9			
6.2. Were notice-triggering data elements involved?	pp. 4 and 9			
6.2.1. First name or first initial and last name, and one or more of the following:	pp. 4 and 9			
6.2.2. Social Security number	pp. 4 and 9			
6.2.3. California Driver's License or Identification Card number	pp. 4 and 9			
6.2.5. Medical information (as defined in 1798.29)	pp. 4 and 10			
6.2.6. Health insurance information (as defined in 1798.29)	pp. 4 and 10			
6.3. Were the notice-triggering data elements acquired, or reasonably believed to have been acquired? ***(Examples only-list is not limited to these***)	p.10			
6.3.1. The information is in the physical possession and control of an unauthorized person, such as a misdirected, lost, or stolen hardcopy document, or file containing notice-triggering information.	p.10			
6.3.2. The information has been viewed, acquired, or copied by an unauthorized person, or a person exceeding the limits of their authorized access.	p.10			
6.3.3. The information was used by an unauthorized person, such as instances of identity theft reported or fraudulent accounts opened.	p.10			
7. Timeliness of Notification	p.10			
7.1. Notification can be sent within ten (10) days from the date data acquisition has been determined.	p.10			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 65D Reference	Yes	No	Notes/Comments
7.2. Notification must be delayed due to legitimate needs of law enforcement	p.10			
7.3. Notification must be delayed to determine scope of breach.	p.10			
7.4. Notification must be delayed to restore system to reasonable integrity.	p.10			
7.5. Delay will or may exacerbate the risk of harm to individuals.	p.10			
7.6. Agency head (or the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf) has authorized the delay of notification.	p.10			
8. Source of Notification	p. 11			
8.1. Agency head (or the senior-level individual designated in writing by the agency head as having authority to act on his/her behalf) will sign the notice.	p. 11			
8.2. The notice is addressed by the entity in which the recipient has a relationship.	p. 11			
8.2. The notice is addressed by an entity in which the recipient has no direct relationship, but the relationship is explained sufficiently in the notice.	p. 11			
9. Content of Notice	pp. 11 and 12			
9.1. The notice leverages the sample notifications provided by OISPP	Appendices B-G			
9.2. The notice is clear and concise.	p. 11			
9.3. The notice uses easy-to-understand language and does not include technical jargon.	p. 11			
9.4. The notice includes a general description of what happened.	p. 11			
9.5. The notice specifically identifies the data elements involved.	p. 11			
9.6. The notice includes the steps the individual can/should take to protect themselves from harm (if any).	p. 12			
9.7. The notice includes an apology.	p. 12			
9.8. The notice includes information about what the agency has done or is doing to investigate the breach, mitigate the losses, and protect against any further breaches.	p. 12			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 65D Reference	Yes	No	Notes/Comments
9.9. The notice includes an individual contact(s) at the agency with the ability to provide more information about the breach to the affected individuals.	p. 12			
9.10. The notice provides a toll-free number for the agency contact, physical address, e-mail address, and postal address if available. If the agency does not have a toll-free number a local number for the contact is provided.	p. 12			
9.11. The agency has knowledge that affected individuals are not English speaking and has prepared notices in the appropriate languages.	p 12			
9.12. The agency has given consideration in providing the notification to individuals who are visually or hearing impaired (e.g., establishing a TDD or posting a large-type notice).	p. 12			
10. Approval of the Notice	pp. 12 and 13			
10.1. Draft notice submitted to OISPP for review an approval by email attachment or facsimile	p. 12			
10.1.1. Communicated with an OISPP representative, immediately prior to submission	p. 12			
10.1.2. Have allowed at least one full business day for OISPP review	p. 13			
10.1.3. Submission marked urgent and includes the required information (subject line OISPP incident tracking number, etc.)	p. 13			
10.2. Final notice submitted to OISPP and includes required information	p. 13			
10.3. The agency has notified and/or sought prior approval for release of notice or the use of reference from other public and private sector agencies that may be impacted by the breach or play a role in mitigating the potential harms (e.g., DMV Fraud Hotline, credit reporting agencies, etc.).	p. 13			
11. Method of Notification	pp. 13 and 14			
11.1. Telephone notification will be made with a concurrent follow-up written by first-class mail	pp. 13 and 14			
11.2. First-class mail notification will be made.	pp. 13 and 14			
11.2.1. Addressed to the named individual.	pp. 13 and 14			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 65D Reference	Yes	No	Notes/Comments
11.2.2. Mailed to the last known address.	pp. 13 and 14			
11.2.3. Mailed separately from other letters and notices.	pp. 13 and 14			
11.2.4. Includes sender or return address information.	pp. 13 and 14			
11.2.5. Labeled on the outside of the envelope to alert recipient to the importance of its contents (e.g., "Important Information Enclosed") as to reduce the likelihood it is mistaken for advertising.	pp. 13 and 14			
11.3. E-mail notification will be made as the following criteria are met:	p.14			
11.3.1. Individual has provided agency with an email address.	p.14			
11.3.2. Individual has provided written consent to use email as the primary means of communication.	p.14			
11.3.3. No known mailing address is available.	p.14			
11.3.4. Email notification is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of Title 15 of the United States Code.	p.14			
11.4. Substitute notification will be made as the following criteria are met:	p.14 and 15			
11.4.1. Agency has demonstrated that more than 500,000 individuals were affected; or the cost of providing notification would exceed $250,000; or the agency does not have adequate contact information on those affected.	p.14			
11.4.2 Substitute notification, as required, will include the following collectively: 1) Conspicuous posting on the agency website; 2) Notification to statewide media; and 3) Email notification when the agency has an email address to individuals. Here, the requirements of section 7001 of Title 15 of the United States Code do not need to be met.	p 14			
11.4.3. Web posting will be made on homepage or a conspicuous link from the homepage.	p.14			
11.4.4. Web posting will also include a link to FAQs	pp.14 and 15			
11.4.5. Information in press release will not impede or compromise the investigation or pose other security risks.	pp.14 and 15			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 65D Reference	Yes	No	Notes/Comments
11.5. Agency has elected to issue press release, as well as first-class notification due to the number of individuals affected.				
11.5.1. Information in press release will not impede or compromise the investigation or pose other security risks.	pp.14 and 15			
12. Preparation for Follow-on Inquiries from Noticed Individuals	pp.15 and 16			
12.1. The agency's public intake areas have been alerted and trained as appropriate to properly direct telephone and in-person inquiries about the breach.	p.15			
12.1.1. Inquiries from the press are to be directed to:	p. 15			
12.1.2. Inquiries from individuals receiving the notice and needing more information are directed to:	p. 15			
12.2. The agency has provisioned for a toll-free call center, staffed with trained personnel.	p. 15			
12.3. The agency has provisioned for documented scripts, and answers to anticipated and frequently asked questions.	pp. 15 and 16			
12.4. The agency has provisioned for a complaint resolution and/or escalation process.	p. 15			
12.5. The agency has provided early warning and information about the timing of notification to all counterparts, so that they are prepared for the potential surge in inquiries.	p. 15			
13. Other Situations When Breach Notification Should be Considered	pp. 16 to 18			
13.1. The agency has considered the nature of any non-notice triggering personal information involved in this breach and the potential harms it poses or may pose to affected individuals.	p. 16			
13.1.1 The agency has determined the nature of the information does potentially pose one or more of the following potential harms ***(Examples only-list is not limited to these***):	p. 16			
13.1.1.1. Harm to reputation.	p. 16			
13.1.1.2. Potential for harassment.	p. 16			
13.1.1.3. Potential for prejudice, particularly when health or financial benefits information is involved.	p. 16			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 65D Reference	Yes	No	Notes/Comments
13.1.1.4. Financial loss.	p. 16			
13.1.1.5. Embarrassment.	p. 16			
13.1.1.6 Legal problems.	p. 16			
13.2. The agency has considered the likelihood that the information has been acquired, or is accessible and usable.	pp. 16 and 17			
13.2.1. The agency has determined it is known or highly likely the information has been acquired and has the potential for misuse by unauthorized persons due to the following ***(examples only-list is not limited to these***):	pp. 16 and 17			
13.2.1.1. The information was not encrypted.	pp. 16 and 17			
13.2.1.2. The encryption product used was not a NIST certified cryptographic module or FIPS-142 validated product.	pp. 16 and 17			
13.3.1.3. The list was posted on the Internet for an extended period of time.	pp. 16 and 17			
13.3. The agency determined there is a likelihood that the breach may lead to harm due to the following ***(examples only-list is not limited to these***):	p. 17			
13.3.1. The individuals affected were victims of stalking or abuse.	p. 17			
13.3.2. The individuals were individuals in high-risk professions, frequently subject to personal threats (e.g., law enforcement, reproductive health care workers, etc.).	p. 17			
13.3.3. The individuals affected were being treated for a highly contagious or infectious disease.	p. 17			
13.3.4. The Social Security number alone can lead to identity theft.	p. 17			
13.4. The ability of the agency to mitigate the risk of harm to individuals.	p.18			
13.4.1. The agency can mitigate further compromise of the system.	p.18			
13.4.2. The agency can monitor systems for misuse of the personal information and patterns of suspicious behavior.	p.18			
13.4.3. The agency has exhausted its ability to mitigate any further risk of harm.	p.18			

Appendix A - Breach Response and Notification Assessment Checklist

Breach Response Requirement or Element	SIMM 65D Reference	Yes	No	Notes/Comments
13.4.4. The apology and assurance of corrective action may serve as a satisfactory remedy those impacted.	p.18			
13.5. The ability of the noticed individual to mitigate the risk to themselves following notification.	p.18			
14. Other Actions Agencies Can Take to Mitigate Harm	p.18			
14.1. The agency has notified financial institutions if state payroll or bank account information was involved.	p.18			
14.2. The agency has notified other agencies about the potential for benefit fraud as applicable (e.g., disability, unemployment, Medi-Cal, etc,)	p.18			
15. Other Considerations When State Employee Data Is Involved				
15.1 Agency has treated affected employees with the same care and concern as any other individual affected by breach.				
15.2. Agency has considered other early warning and notification methods to augment the first-class mail notification (e.g., such as email, Intranet posting, townhall meetings)				
15.3. Agency has notified managers and supervisors of the affected employees and adequately prepared them to answer questions from employees.				
15.4. Agency has considered notifying represented employee organizations as may be appropriate.				
15.5. Agency has considered the use of townhall meetings to respond to employee questions and concerns following notification				
16. Other Considerations From a Public Relations Perspective	p. 19			
16.1. The agency has considered advanced notification to the media.	p. 19			
16.2. The agency has considered acquiring credit monitoring services for the affected individuals. Note: This should only be considered when the incident involves SSN and/or CDL.	p. 19			

B. APPENDIX B: Sample Breach Notice: Social Security Number

[*Salutation*]

We are writing to you because of a recent security incident at [*name of organization*].

[*Describe what happened in general terms, specifically what kind of personal information was involved, and what you are doing in response*.]

To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files by following the recommended privacy protection steps outlined in the enclosure.

For more information on identity theft, you may visit the Web site of the California Office of Information Security and Privacy Protection at www.privacy.ca.gov

We regret that this incident occurred and want to assure you that we are reviewing and revising our procedures and practices to minimize the risk of recurrence. Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Closing*]

Enclosure [*Enclose the Security Breach - First Steps Enclosure*]

C. APPENDIX C: Sample Breach Notice - Driver's License or California ID Card Number

[*Salutation*]

We are writing to you because of a recent security incident at [*name of organization*].

[*Describe what happened in general terms, specifically what kind of personal information was involved, and what you are doing in response.*]

Since your Driver's License [*or California Identification Card*] number was involved, we recommend that you call the toll-free DMV Fraud Hotline at 866-658-5758 to report the [*loss or theft*].

To further protect yourself, we recommend that you place a fraud alert on your credit files by following the recommended privacy protection steps outlined in the enclosure.

For more information on identity theft, you should visit the Web site of the California Office of Information Security and Privacy Protection at www.privacy.ca.gov

We regret that this incident occurred and want to assure you we are reviewing and revising our procedures and practices to minimize the risk of recurrence. Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Closing*]

Enclosure [*Enclose the Security Breach - First Steps Enclosure*]

D. APPENDIX D: Sample Breach Notice - Credit Card Number or Financial Account Number

[*Salutation*]

We are writing to you because of a recent security incident at [*name of agency*].

[*Describe what happened in general terms, specifically what type of personal information was involved, and what you are doing in response*].

To help prevent unauthorized access and fraudulent activity on this account, we recommend that you immediately contact *[the credit card or financial account issuer*] and close your account Tell them that your account may have been compromised, and ask that they report it as "closed at customer request."

If you want to open a new account, ask your account issuer to give you a PIN or password associated with the new account. This will help control access to the account.

We have enclosed additional privacy protection recommendations, and for more information on identity theft, you should visit the Web site of the California Office of Information Security and Privacy Protection at www.privacy.ca.gov

We regret that this incident occurred and want to assure you we are reviewing and revising our procedures and practices to minimize the risk of recurrence. Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Closing*]

Enclosure [*Enclose the Security Breach - First Steps Enclosure*]

E. APPENDIX E: Sample Breach Notice - Medical Information Only*

[*Salutation*]

We are writing to you because of a recent security incident at [*name of organization*].

[*Describe what happened in general terms, specifically what kind of personal information was involved, and what you are doing in response. If the breach does not involve Social Security number, driver's license/California Identification Card, or financial account numbers, say so. Refer to the following language.*]

Please note, the information was limited to [*specify, (e.g., your name and medical treatment)*] and did not contain any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. Nonetheless, we felt it necessary to inform you since your medical information [*or medical history, medical condition, or medical treatment or diagnosis*] was involved.

We recommend that you regularly review the explanation of benefits statement that you receive from [*us, your health insurance plan, or your health insurer*]. If you see any service that you believe you did not receive, please contact [*us, your health insurance plan, your health insurer*] at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. You can order your reports from the three credit reporting agencies for free each year by calling 1-877-322-8228 or going to the Annual Credit Report website at www.annualcreditreport.com

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [*provider or plan*], to serve as a baseline. For information about your medical privacy rights, we recommend you visit the website of the California Office of Information Security and Privacy Protection at www.privacy.ca.gov

We regret that this incident occurred and want to assure you we are reviewing and revising our procedures and practices to minimize the risk of recurrence. Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Closing*]

* Additional language will be necessary if other notice triggering information was involved.

F. APPENDIX F: Sample Breach Notice - Health Insurance Information Only*

[*Salutation*]

We are writing to you because of a recent security incident at [*name of organization*].

[*Describe what happened in general terms, specifically what kind of personal information was involved, and what you are doing in response. If the breach does not involve Social Security number, driver's license/California Identification Card, or financial account numbers, say so. Refer to the following language.*]

Please note, the information was limited to [*specify, (e.g., your name and medical treatment)*] and did not contain any other information, such as Social Security number, Driver's License number, or financial account numbers which could expose you to identity theft. Nonetheless, we felt it necessary to inform you since your health insurance information [*or policy, plan number, or subscriber identification number*] was involved.

We recommend that you regularly review the explanation of benefits statement that you receive from [*us, your health insurance plan, or your health insurer*]. If you see any service that you believe you did not receive, please contact [*us, your health insurance plan, your health insurer*] at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. You can order your reports from the three credit reporting agencies for free each year by calling 1-877-322-8228 or going to the Annual Credit Report website at www.annualcreditreport.com

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [*provider or plan*], to serve as a baseline. For information about your medical privacy rights, we recommend you visit the website of the California Office of Information Security and Privacy Protection at www.privacy.ca.gov

We regret that this incident occurred and want to assure you we are reviewing and revising our procedures and practices to minimize the risk of recurrence. Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Closing*]

* Additional language will be necessary if other notice triggering information was involved.

G. APPENDIX G: Sample Breach Notice – Hybrid (SSN and Health Information)

[*Salutation*]

We are writing to you because of a recent security incident at [*name of organization*].

[*Describe what happened in general terms, specifically what kind of personal information was involved, and what you are doing in response*.]

Because your Social Security number was involved, and in order to protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files and order copies of your credit reports by following the recommended privacy protection steps outlined in the enclosure. Check your credit reports for any accounts or medical bills that you do not recognize. If you find anything suspicious, follow the instructions found in step four of the enclosure.

Since your health insurance information [*or policy, plan number, or subscriber identification number*] was also involved, we recommend that you regularly review the explanation of benefits statement that you receive from [*us, your health insurance plan, or your health insurer*]. If you see any service that you believe you did not receive, please contact [*us, your health insurance plan, your health insurer*] at the number on the statement [*or provide a number here*]. If you do not receive regular explanation of benefits statements, contact your provider or plan and ask them to send such statements following the provision of services provided in your name or under your plan number.

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your [*provider or plan*], to serve as a baseline. For more information about privacy protection steps and your medical privacy rights, we recommend you visit the website of the California Office of Information Security and Privacy Protection at www.privacy.ca.gov

We regret that this incident occurred and want to assure you we are reviewing and revising our procedures and practices to minimize the risk of recurrence. Should you need any further information about this incident, please contact [*name of the designated agency official or agency unit handling inquiries*] at [*toll-free phone number*].

[*Closing*]

Enclosure [*Enclose the Security Breach - First Steps Enclosure*]

H. APPENDIX H: Security Breach - First Steps Enclosure (English)

This document is available on the OISPP Web site at
http://www.oispp.ca.gov/consumer_privacy/pdf/Security_Breach_First_Steps.pdf

CALIFORNIA
OFFICE OF
PRIVACY
PROTECTION

www.privacy.ca.gov

Privacy Protection Recommendations

What to Do If Your Personal Information Is Compromised

1 Contact the three credit bureaus.

You can report the potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus. You will also be sent instructions on how to get a copy of your report from each of the credit bureaus. As a possible victim of identity theft, you will not be charged for these copies.

Trans Union 1-800-680-7289 Experian 1-888-397-3742 Equifax 1-800-525-6285

2 What it means to put a fraud alert on your credit file.

A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that there may be fraud on the account. This alerts the merchant to take steps to verify the identity of the applicant. A fraud alert lasts 90 days and can be renewed.

3 Review your credit reports. Look through each one carefully.

Look for accounts you don't recognize, especially accounts opened recently. Look in the inquiries section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. You may find some inquiries identified as "promotional." These occur when a company has obtained your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (You are automatically removed from lists to receive unsolicited offers of this kind when you place a fraud alert.) Also, as a general precaution, look in the personal information section for any address listed for you where you've never lived.

4 If you find items you don't understand on your report, call the credit bureau at the number on the report.

Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved and report the crime to your local police or sheriff's office. For more information on what to do in this case, visit the California Office of Privacy Protection's Web site at www.privacy.ca.gov, and go to the Identity Theft page.

CALIFORNIA OFFICE OF INFORMATION SECURITY & PRIVACY PROTECTION
www.oispp.ca.gov

I. APPENDIX I: Security Breach - First Steps Enclosure (Spanish)

This document is available on the OISPP Web site at
http://www.oispp.ca.gov/consumer_privacy/pdf/Security_Breach_First_Steps_SP.pdf

CALIFORNIA
OFFICE OF
PRIVACY
PROTECTION

www.privacy.ca.gov

Cómo proteger su privacidad

Qué hacer si su información personal está comprometida

1 Póngase en contacto con las tres agencias de crédito.

Para informar el robo potencial de su identidad llame sin cargo a cualquiera de las tres agencias principales de crédito indicados a continuación. Accederá a un sistema telefónico automatizado para informar fraude el cual le permitirá marcar su archivo de crédito en las tres agencias de crédito con un alerta de fraude. También le enviarán instrucciones para solicitar una copia de su informe de cada una de las agencias de crédito. No tendrá que pagar por las copias del informe ya que se trata de un posible robo de identidad.

Trans Union 1-800-680-7289 Experian 1-888-397-3742 Equifax 1-800-525-6285

2 Qué quiere decir poner un alerta de fraude en su archivo de crédito.

Un alerta de ayudará a protegerlo contra la posibilidad de que un ladrón de identidad abra cuentas nuevas de crédito en su nombre. Cuando un comerciante verifica el historial de crédito de una persona que está solicitando crédito, recibirá un aviso indicando que puede haber fraude en la cuenta. Esto alerta al comerciante a que tome pasos para verificar la identidad del solicitante. El alerta de fraude dura 90 días y se puede renovar.

3 Examine sus informes de crédito. Revise cuidadosamente cada uno de ellos.

Fíjese si hay cuentas que no reconoce, sobre todo cuentas abiertas recientemente. Fíjese en la sección de consultas para ver si hay empresas a las que no les solicitó crédito. Algunas empresas facturan bajo un nombre distinto que el nombre de la empresa. En esos casos, la agencia de crédito podrá aclarar de qué empresa se trata. Puede encontrar ciertas consultas identificadas como "promocionales". Estas consultas son efectuadas cuando una compañía obtuvo su nombre y dirección de una agencia de crédito y le envía una oferta de crédito. Las consultas promocionales no son un signo de fraude. (Cuando haga un alerta de fraude, lo eliminarán automáticamente de las listas de ofertas no solicitadas de este tipo). Como precaución general, fíjese también en la sección sobre información personal para ver si hay alguna dirección donde nunca ha vivido.

4 Si encuentra en su informe transacciones que no comprende, llame a la agencia de crédito al número que aparece en el informe.

El personal de la agencia de crédito analizará el informe junto con usted. Si no puede explicar la información usted tendrá que llamar a los acreedores involucrados e informar el delito en su comisaría u oficina del alguacil local. Para obtener más información sobre lo que tiene que hacer en este caso, visite el sitio Web de la Oficina de Protección de Privacidad de California en www.privacy.ca.gov y vaya a la página de Robo de identidad *(Identity Theft)*.